PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

COMMUNICATION OF
INTERNATIONAL APPLICATIONS

(PCT Article 20)

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as designated Office

Date of mailing:
03 April 2000 (03.04.00)

The International Bureau transmits herewith copies of the international applications having the following international application numbers and international publication numbers:

International application no.:	International publication no.:
PCT/JP99/04328	

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

特　許　協　力　条　約

EP US PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　99-F-037PCT	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０４３３６	国際出願日 (日.月.年)　１１．０８．９９	優先日 (日.月.年)　１２．０８．９８
出願人（氏名又は名称） 森永乳業株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
- ☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
- ☐ この国際出願に含まれる書面による配列表
- ☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
- ☐ 出願後に、この国際調査機関に提出された書面による配列表
- ☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
- ☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
- ☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
- ☒ 出願人が提出したものを承認する。
- ☐ 次に示すように国際調査機関が作成した。

５．要約は
- ☒ 出願人が提出したものを承認する。
- ☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第 ＿＿＿＿ 図とする。
- ☐ 出願人が示したとおりである。
- ☐ 出願人は図を示さなかった。
- ☐ 本図は発明の特徴を一層よく表している。
- ☒ なし

国際調査報告

国際出願番号 PCT／ＪＰ９９／０４３３６

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int. Cl[6] A61K31／66, 31／195, 38／01, 38／16, 38／40,
35／78, 31／23, 31／20, 31／70, 33／00

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int. Cl[6] A61K31／66, 31／195, 38／01, 38／16, 38／40,
35／78, 31／23, 31／20, 31／70, 33／00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
CAPLUS（STN）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ，１－１２８９１９，Ａ（雪印乳業株式会社） １．５月．１９８９（２２．０５．８９） 全文（ファミリーなし）	１－３

☐ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０５．１１．９９	16.11.99

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	４Ｃ	９８４１
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	森井　隆信　印 電話番号　０３－３５８１－１１０１　内線　６４６０		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

特　許　協　力　条　約

PCT

US

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号　ＰＣＴ００１ＪＳＴ	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０４３２８	国際出願日 （日.月.年）　１０．０８．９９	優先日 （日.月.年）　２４．０９．９８
出願人（氏名又は名称） 平野　琢也		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　1　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報[redacted]　　国際出願番号[redacted]CT／JP99／04328

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶　　H04L9／38, H04B10／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁶　　H04L9／38, H04B10／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996
日本国公開実用新案公報	1971－1999
日本国登録実用新案公報	1994－1999
日本国実用新案登録公報	1996－1999

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	M. J. Werner, G. J. Milburn; "Eavesdropping using quanturn-nondemolition measurements", PHYSICAL REVIEW A, Vol. 47, No. 1 (1993) p. 634-641	1, 5, 8-11
Y		12-14
A		2-4, 6, 7
Y	H. Bartelt, K.-H. Brenner; "The Wigner Distribution Function An Alternate Signal Representation in Optics", ISRAEL Journal of TECHNOLOGY, Vol. 18, No. 5 (1980) p. 260-262	12

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　02. 11. 99	国際調査報告の発送日　16.11.99
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5W　4229 青木　重徳　印 電話番号　03－3581－1101　内線　3576

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	副島俊雄, 貝淵俊二 著;新版・光ﾌｧｲﾊﾞ通信 株式会社電気通信技術ﾆｭｰｽ社 発行, (12.12.1981) p.252-253	13, 14
A	C.Marand, P.D.Townsend; "Quantum key distribution over distances as long as 30km.", Optics Letter, Vol.20, No.12 (1995) p.1695-1697	1-14
A	Yi Mu, Yuliang Zheng, Yan-Xia Lin; "Multi-User Quantum Cryptography", International Symposium on Information Theory & Its Application 1994, Vol.1 (1994) p.245-250	1-14
A	B.A.Slutsky, R.Rao, P.-C.Run, Y.Fainman; "Security of cryptography against individual attacks", PHYSICAL REVIEW A, Vol.57, No.4 (1998) p.2383-2390	1-14
A	松枝秀明; "量子暗号の現状と期待", 電子情報通信学会誌, Vol.81, No.3(25.03.1998) p.225-228	1-14

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PCT001JST	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP99/04328	International filing date (*day/month/year*) 10 August 1999 (10.08.99)	Priority date (*day/month/year*) 24 September 1998 (24.09.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/38, H04B 10/00		
Applicant HIRANO, Takuya		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 August 1999 (10.08.99)	20 April 2000 (20.04.2000)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP99/04328

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☐ the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the drawings:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/JP99/04328

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	2-4,6,7,12-14	YES
	Claims	1,5,8-11	NO
Inventive step (IS)	Claims	2-4,6,7	YES
	Claims	1,5,8-14	NO
Industrial applicability (IA)	Claims	1-14	YES
	Claims		NO

2. Citations and explanations

Claims 1, 5, 8 through 11

Document 1 (Werner, M.J., G.J. Milburn, "Eavesdropping using quantum-nondemolition measurements," PHSYICAL REVIEW A, Vol. 47, No. 1 (1993), p. 639-641) describes, in quantum cryptocommunciation using optical signals, art for detecting eavesdropping based on the quantum mechanical probability distribution of the difference signal of the signal light. The inventions described in claims 1, 5, and 8 through 11 constitute a portion of the art described in document 1, and thus do not appear to possess novelty.

Claim 12

Document 2 (Bartelt, H., Brenner, K.H., "The Wigner Distribution Function: An Alternate Signal Representation in Optics," Israel Journal of Technology, Vol. 18, No. 5, p. 260-262) describes art using the Wigner distribution function as a method of representation in optical telecommunications. It would be obvious for a party skilled in the art to use the optical signal representation method of the Wigner distribution function described in document 2 as the representation method of the probability distribution of the difference signal of the signal light described in document 1.

Claims 13, 14

Document (Fukushima, S., Kaibuchi, S., "Shinpan: Tsuu-fibaa Tsuushin," Kabushiki Kaisha Denkitsuushin Gijutsu Nyuusu Sha (12 December 1981), p. 252-3) states that when such photo diodes as photo diodes made of silicon (Si) and photo diodes made of InGaAs are used as an element to convert optical signals into electricity, the transmission wavelength is 0.8 to 0.9 μm when a silicon photo diode is used, and is 1.1 to 1.7 μm when an InGaAs photo diode is used. It would be obvious to a party skilled in the art to use a photo diode made from the respective materials corresponding to the respective wavelengths as described in document 3 as the signal light receiving optical element for optical telecommunications described in document 1.

Claims 2 through 4, 6 and 7

Document 4 (Marand, C., Townsend, P.D., "Quantam key distribution over distances as long as 30 km.," Optics Letters, Vol. 20, No. 12 (1995), p. 1695-1697) is a document indicating the general state of the art in the relevant technical field. It describes art for the stable transmission of a cipher key using an interference measurement quantum cryptography scheme. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunciation system wherein optical signals are separated into intense reference signals and weak transmission signals.

Document 4 (Yi Mu, Yuliang Zheng, Yan-Xia Lin, "Multi-User Quantum Cryptography," International Symposium on Information Theory & Its Application," Vol. 1. (1994), p. 245-250) is a document indicating the general state of the art in the relevant technical field. It describes the detection within a prescribed sphere of correlation with information of eavesdropping by interrupt/resend against a cipher common key transmission protocol based on the

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of Box V (Citations and explanations):

uncertainty principle of quantum mechanics. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunciation system wherein optical signals are separated into intense reference signals and weak transmission signals.

Document 5 (Slutsky, B.A., Rao. R., Run, P.C., Fainman, Y., "Security of quantum cryptography against individual attacks." PHYSICAL REVIEW A, Vol. 57, No. 4 (1998), p. 2383-2398) is a document indicating the general state of the art in the relevant technical field. It describes (1) examination in two-condition or four-condition quantum cryptography protocol of the relationship between transmission error and the maximum volume of information that an eavesdropper is capable of extracting and (2) how said quantum cryptography protocol defends against all attacks when the optimal eavesdropping method in each case is made clear and the eavesdropping strategy is restricted so that each bit of the quantum transmission can be attacked individually. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunciation system wherein optical signals are separated into intense reference signals and weak transmission signals.

Document 6 (Matsugi, S., "Ryoushi angou no genjou to kitai," Denshi Jouhou Tsuushin Gakkai Shi, Vol. 81, No.3 (25.03.1998), P. 225-228) is a document indicating the general state of the art in the relevant technical field. It describes quantum cryptography capable of detecting the eavesdropping of ciphers using the exclusivity of a conjugate pair, by using a pair of conjugate physical amount and quantum cryptography that uses natural emissions to control the natural emission of optical particles by adjusting the size and material of cavities. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunciation system wherein optical signals are separated into intense reference signals and weak transmission signals.

特　許　協　力　条　約

PCT

国際予備審査報告

(法第１２条、法施行規則第56条)
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　ＰＣＴ００１ＪＳＴ	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０４３２８	国際出願日 (日.月.年)　１０．０８．９９	優先日 (日.月.年)　２４．０９．９８
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ'　Ｈ０４Ｌ９／３８，Ｈ０４Ｂ１０／００		
出願人（氏名又は名称） 平野　琢也		

１．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．　この国際予備審査報告は、この表紙を含めて全部で　4　ページからなる。

☐ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で＿＿＿＿＿＿ページである。

３．　この国際予備審査報告は、次の内容を含む。

Ⅰ ☒ 国際予備審査報告の基礎

Ⅱ ☐ 優先権

Ⅲ ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成

Ⅳ ☐ 発明の単一性の欠如

Ⅴ ☒ ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明

Ⅵ ☐ ある種の引用文献

Ⅶ ☐ 国際出願の不備

Ⅷ ☐ 国際出願に対する意見

国際予備審査の請求書を受理した日　１０．０８．９９	国際予備審査報告を作成した日　２０．０４．００
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｗ　４２２９ 青木　重徳　印 電話番号　０３－３５８１－１１０１　内線　３５７４

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０４３２８

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。ＰＣＴ規則70.16, 70.17）

☒ 出願時の国際出願書類

☐ 明細書　第 ＿＿＿＿＿＿＿＿ ページ、　出願時に提出されたもの
明細書　第 ＿＿＿＿＿＿＿＿ ページ、　国際予備審査の請求書と共に提出されたもの
明細書　第 ＿＿＿＿＿＿＿＿ ページ、　＿＿＿＿＿＿＿＿ 付の書簡と共に提出されたもの

☐ 請求の範囲　第 ＿＿＿＿＿＿＿＿ 項、　出願時に提出されたもの
請求の範囲　第 ＿＿＿＿＿＿＿＿ 項、　ＰＣＴ１９条の規定に基づき補正されたもの
請求の範囲　第 ＿＿＿＿＿＿＿＿ 項、　国際予備審査の請求書と共に提出されたもの
請求の範囲　第 ＿＿＿＿＿＿＿＿ 項、　＿＿＿＿＿＿＿＿ 付の書簡と共に提出されたもの

☐ 図面　第 ＿＿＿＿＿＿＿＿ ページ／図、　出願時に提出されたもの
図面　第 ＿＿＿＿＿＿＿＿ ページ／図、　国際予備審査の請求書と共に提出されたもの
図面　第 ＿＿＿＿＿＿＿＿ ページ／図、　＿＿＿＿＿＿＿＿ 付の書簡と共に提出されたもの

☐ 明細書の配列表の部分　第 ＿＿＿＿＿＿＿＿ ページ、　出願時に提出されたもの
明細書の配列表の部分　第 ＿＿＿＿＿＿＿＿ ページ、　国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分　第 ＿＿＿＿＿＿＿＿ ページ、　＿＿＿＿＿＿＿＿ 付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である ＿＿＿＿＿＿＿＿ 語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。
☐ 明細書　第 ＿＿＿＿＿＿＿＿ ページ
☐ 請求の範囲　第 ＿＿＿＿＿＿＿＿ 項
☐ 図面　図面の第 ＿＿＿＿＿＿＿＿ ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０４３２８

Ⅴ．　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）　請求の範囲　２－４，６，７，１２－１４　有
請求の範囲　１，５，８－１１　無

進歩性（ＩＳ）　請求の範囲　２－４，６，７　有
請求の範囲　１，５，８－１４　無

産業上の利用可能性（ＩＡ）　請求の範囲　１－１４　有
請求の範囲　　無

２．　文献及び説明（ＰＣＴ規則70.7）

請求の範囲１，５，８－１１
文献１：M.J.Werner, G.J.Milburn; "Eavesdropping using quantum-nondemolition measurements", PHYSICAL REVIEW A, Vol.47, No.1 (1993) p.639-641
には、光信号を用いる量子暗号通信において、信号光の差信号における量子力学的な確率分布の変化に基づいて盗聴を検出する技術が記載されており、請求の範囲１，５，８－１１に記載された発明は、上記文献１に記載された技術の一部をなすものであり、新規性を有しない。

請求の範囲１２
文献２：H.Bartelt, K.-H.Brenner; "The Wigner Distribution Function An Alternate Signal Representation in Optics", ISRAEL Journal of TECHNOLOGY, Vol.18, No.5 (1980) p.260-262
には、光通信における信号の表現方法としてウィグナー分布関数を用いる技術が記載されており、文献１に記載されている信号光の差信号における確率分布の表現方法として、文献２に記載されているウィグナー分布関数による光信号の表現方法を用いることは、当技術分野の専門家にとっては自明である。

請求の範囲１３，１４
文献３：副島俊雄，貝淵俊二 著；新版・光ﾌｧｲﾊﾞ通信 株式会社電気通信技術ﾆｭｰｽ社 発行，(12.12.1981) p.252-253
には、光信号を電気に変換する素子としてシリコン（Ｓｉ）を材料としたフォトダイオードやＩｎＧａＡｓを材料としたフォトダイオードが用いられ、その伝送波長はシリコンフォトダイオードを用いた場合は０．８－０．９μｍ、ＩｎＧａＡｓフォトダイオードを用いた場合は１．１－１．７μｍである旨が記載されており、文献１に記載されている光通信の信号光受光素子として文献２に記載されている各波長に対応した各材料からなるフォトダイオードを用いることは、当技術分野の専門家にとっては自明のものである。

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第Ｖ．２欄の続き

請求の範囲２－４，６，７

文献３：C. Marand, P. D. Townsend; "Quantum key distribution over distances as long as 30km.", Optics Letter, Vol. 20, No. 12 (1995) p. 1695-1697

は、当該技術分野における一般的技術水準を示す文献であって、干渉測定量子暗号スキームを用いる暗号キーの安全な伝送技術が記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献１－６のいずれにも記載も示唆もされていない。

文献４：Yi Mu, Yuliang Zheng, Yan-Xia Lin; "Multi-User Quantum Cryptography", International Symposium on Information Theory & Its Application 1994, Vol. 1 (1994) p. 245-250

は、当該技術分野における一般的技術水準を示す文献であって、量子物理学の不確定性原理に基づく暗号共通鍵配送プロトコルに対して、割込／再送による盗聴が情報と相関の定式化範囲内で検出できることが記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献１－６のいずれにも記載も示唆もされていない。

文献５：B. A. Slutsky, R. Rao, P.-C. Run, Y. Fainman; "Security of quantum cryptography against individual attacks", PHYSICAL REVIEW A, Vol. 57, No. 4 (1998) p. 2383-2398

は、当該技術分野における一般的技術水準を示す文献であって、伝送誤りと盗聴者が引き出しうる最大情報量の関係を二状態及び四状態の量子暗号プロトコルにて検討するとともに、各場合における最適盗聴法を明示し、盗聴戦略を量子伝送の各ビットが個別独立的に攻撃されるように限定した場合、前記量子暗号プロトコルは全ての攻撃に対抗できることが記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献１－６のいずれにも記載も示唆もされていない。

文献６：松枝秀明; "量子暗号の現状と期待", 電子情報通信学会誌, Vol. 81, No. 3 (25. 03. 1998) p. 225-228

は、当該技術分野における一般的技術水準を示す文献であって、物理量の共役な組を用い、共役な組の排他性を利用して暗号の盗聴を検知可能とする量子暗号と、キャビティのサイズや媒質を調整することにより光子の自然放出を制御することで、自然放出を利用した量子暗号が記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献１－６のいずれにも記載も示唆もされていない。

記録原本

特許協力条約に基づく国際出願願書 PCT001JST
原本（出願用）- 印刷日時 1999年08月10日（10.08.1999）火曜日 14時08分18秒

0 0-1	受理官庁記入欄 国際出願番号	PCT/JP99/04328
0-2	国際出願日	10.08.99
0-3	（受付印）	PCT International Application 日本国特許庁
0-4 0-4-1	この特許協力条約に基づく国際出願願書(様式 - PCT/RO/101)は、 右記によって作成された。	PCT-EASY Version 2.83 (updated 01.03.1999)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁（RO/JP）
0-7	出願人又は代理人の書類記号	PCT001JST
I	発明の名称	量子暗号通信システム
II II-1 II-2	出願人 この欄に記載した者は 右の指定国についての出願人である。	出願人及び発明者である（applicant and inventor） すべての指定国（all designated States）
II-4ja	氏名(姓名)	平野 琢也
II-4en	Name (LAST, First)	HIRANO, Takuya
II-5ja	あて名:	169-0075 日本国 東京都 新宿区高田馬場 ２－１－１－１４０３
II-5en	Address:	2-1-1-1403, Takadanobaba, Shinjuku-ku, Tokyo 169-0075 Japan
II-6	国籍（国名）	日本国 JP
II-7	住所（国名）	日本国 JP
II-8	電話番号	03-3232-0950
II-9	ファクシミリ番号	03-3232-0950
II-10	電子メール	takuya.hirano@gakushuin.ac.jp

特許協力条約に基づく国際出願願書 PCT001JST
原本（出願用）- 印刷日時 1999年08月10日（10.08.1999）火曜日 14時08分18秒

IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人（agent）
IV-1-1ja	氏名(姓名)	平山 一幸
IV-1-1en	Name (LAST, First)	HIRAYAMA, Kazuyuki
IV-1-2ja	あて名:	160-0004 日本国 東京都 新宿区四谷 ４－３２－８ ＹＫＢサニービル６階
IV-1-2en	Address:	YKB-Sunny Bldg. 6F 32-8, Yotsuya 4-chome, Shinjuku-ku, Tokyo 160-0004 Japan
IV-1-3	電話番号	03-3352-1808
IV-1-4	ファクシミリ番号	03-3352-2150
IV-1-5	電子メール	PED01452@nifty.ne.jp
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	--
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	US
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。	
V-6	指定の確認から除かれる国	なし（NONE）
VI-1	先の国内出願に基づく優先権主張	
VI-1-1	先の出願日	1998年09月24日（24.09.1998）
VI-1-2	先の出願番号	平成１０年特許願第２７０１４９号
VI-1-3	国名	日本国 JP
VI-2	優先権証明書送付の請求 上記の先の出願のうち、右記の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁に対して請求している。	VI-1
VII-1	特定された国際調査機関(ISA)	日本国特許庁（ISA/JP）

特許協力条約に基づく国際出願願書 PCT001JST

原本（出願用）- 印刷日時 1999年08月10日（10.08.1999）火曜日 14時08分18秒

VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	3	-
VIII-2	明細書	14	-
VIII-3	請求の範囲	3	-
VIII-4	要約	1	pct001jst.txt
VIII-5	図面	7	-
VIII-7	合計	28	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	優先権書類送付請求書	-
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-17	その他	国際事務局の口座への振込を証明する書面	-
VIII-18	要約書とともに提示する図の番号	1	
VIII-19	国際出願の使用言語名:	日本語（Japanese）	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	平山 一幸	

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	10.08.99
10-2 10-2-1 10-2-2	図面： 受理された 不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	23 AUGUST 1999 (23.08.99)

明　細　書

量子暗号通信システム

技術分野

この発明は、通信の安全性を確保するための秘密鍵の配布に利用され、特に伝送信号の量子力学的な状態を測定し、実質的に高い量子効率で伝送信号の検出をするための量子暗号通信システムに関する。

背景技術

通信の安全性を確保するための従来の暗号技術には、正規の通信者のみが知っている共通の秘密鍵を用いる秘密鍵暗号方式と、秘密鍵と公開鍵という一対の鍵を用いる公開鍵暗号方式とがある。

公開鍵暗号方式の暗号は、その秘蔵性を、例えば非常に大きな整数の因数分解が計算困難であるといったことに拠っているが、計算機の性能の進歩やネットワークを使った分散処理技術の発達等によりその安全性は必ずしも万全とはいえない。

これに対して、正規の通信者のみが知っている秘密鍵を送り手と受け手のみで共有することができれば絶対的に安全な通信が可能になる。このような中で、最近、秘密鍵の配布方法の秘蔵性を量子力学の原理にもとめる通信方法である量子暗号が提案されている（Ｊ．Ｃｒｙｐｔｏｌｏｇｙ、５、３－２８（１９９２）Ｃ．Ｈ．Ｂｅｎｎｅｔｔ　ｅｔａｌ）。

量子力学の原理によれば、測定行為は必然的に被測定対象に擾乱を与えるので、盗聴者による盗聴の試みは必ず信号に変化を与える。

したがって、信号の変化を監視することにより盗聴者の存在を暴くことができる。つまり、量子暗号を用いると距離的に離れた２点間で秘蔵性の非常に高い秘密鍵を共有することができる。従来の量子暗号は伝送信号の担い手として光を用い、かつ、光の検出に光子計数法を用いている。光子計数法とは１個以上の光子が検出器に入射したとき、ある確率（量子効率という）で電気パルスが発生する

光の検出方法である。

しかしながら、このような従来の方法では、光の検出に光子計数法を用いているため、そのことに起因する原理的及び技術的な解決すべき課題がある。

まず、原理的な課題は、伝送された後の信号の量子力学的な状態を調べることが出来ないので、盗聴者が量子非破壊測定等の高度な手段をとった場合、それを検知することができない。すなわち、盗聴者が光子数の情報を信号の光子数に変化を与えずに読み出すことが可能なので（測定の影響は位相の変化に現れる）、伝送後の光子数のみを測定していても盗聴に気がつかないことになる。

さらに技術的な課題として、光通信で通常用いられる１．３μｍや１．５μｍの光に対して、高い量子効率を有する検出器が現存しないことがある。検出の際の損失はデータの転送レートを低下させるだけでなく、原理的には盗聴者による盗聴の試みと区別できない。

そこで、この発明は、伝送信号の量子力学的な状態の測定が可能になるとともに、実質的に高い量子効率で伝送信号の検出が可能な量子暗号通信システムを提供することを目的とする。

発明の開示

この目的を達成するために、本発明の量子暗号通信システムは、光信号を用いる量子暗号通信において、盗聴の操作によって生じる信号光の差信号における振幅と位相とで規定される量子力学的な確率分布の変化に基づいて盗聴を検出することを特徴とする。

このような構成により、伝送信号の量子状態をモニターすることによって従来は困難であった量子非破壊測定のような高度な盗聴を検出することができる。

また本発明の量子暗号通信システムは、量子暗号通信において、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で参照信号と伝送信号とに位相差を付与し、これら２つの信号を受信側で重ね合わせ、得られる相互に逆位相の関係にある２つの出力光の差を求め、伝送信号の量子状態の揺らぎに依存した出力光の差の頻度分布に基づいて送信側と受信側との秘密鍵を共有するとともに、伝送信号の量子状態の揺ら

ぎを直接測定することを特徴とするものである。

このような構成によって、参照信号の強度が強いことにより、理論的な上限に近い効率で伝送信号を検出することができる。

また本発明の量子暗号通信システムは、光源からの光を伝送信号と参照信号とに分割する第１のビームスプリッターと、伝送信号に位相変調を与える位相変調手段と、伝送信号を量子力学的な状態変化で検出できる微弱な信号にする光減衰器と、参照信号に位相変調を与える位相変調手段とを備え、位相変調した微弱な伝送信号と位相変調した強度の強い参照信号とを重ね合わせて出力する第２のビームスプリッターと、第２のビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有するものである。

このような構成により、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で参照信号と伝送信号とに位相差を付与し、これら２つの信号を受信側で重ね合わせ、得られる相互に逆位相の関係にある２つの出力の差を求め、伝送信号の量子状態の揺らぎに依存した出力の差の頻度分布に基づいて送信側と受信側の秘密鍵を共有し、伝送信号の量子状態の揺らぎを測定する。したがって、高効率の検出ができるとともに信号光の量子状態を測定することができる。

この発明は、好ましくは、上記位相変調手段が入射する光の波長程度の微小な距離を移動可能にした鏡を含んでなる。このような構成により位相変調を容易にすることができる。

また、本発明の量子暗号通信システムは、好ましくは、参照信号と伝送信号とを時間及び偏光状態で分離して同一の経路を伝送している。このような構成により、伝送路として１本の光ファイバーで伝送するので、長距離の量子暗号通信システムを提供することができる。

さらに本発明の量子暗号通信システムは、光源からの光を伝送信号と参照信号とに分割する第１のビームスプリッターと、伝送信号を一方の長い経路を通し偏光する第１の偏光素子と、伝送信号を量子力学的な状態で検出できる微弱な信号にする光減衰器と、伝送信号に所定の位相変調を与える第１の位相変調手段と、

他方の短い経路に通した強度の強い参照信号と伝送信号とを同一光軸上に戻す第１の偏光ビームスプリッターとを備え、一本の光ファイバーを伝送してきた伝送信号及び参照信号を分離する第２の偏光ビームスプリッターと、分離した伝送信号を一方の短い経路に通し位相変調を与える第２の位相変調手段と、分離した参照信号を他方の長い経路に通し偏光する第２の偏光素子とを有しており、時間及び偏光状態が一致した伝送信号と参照信号とを重ね合わせて出力する第２のビームスプリッターと、第２のビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有するものである。

このような構成により、伝送信号と参照信号とが異なる経路を進むのは送信者と受信者側の短い距離だけで、大部分の伝送路は同一の経路を進むので、長距離の量子暗号伝送であっても２つの光の相対的な光路差の変動を小さくすることができる。

本発明の量子暗号通信システムは、好ましくは、前記光ファイバーの出力側に参照信号の偏光の乱れを補正する第３の偏光素子が設けられる。

このような構成により、光ファイバー伝送中の偏光の乱れを強度の強い参照信号で行うので、偏光の乱れを効果的に補正することができる。

さらに本発明の量子暗号通信システムは、好ましくは、出力光の差の信号に正負それぞれにしきい値を設定し、このしきい値を基準にして伝送信号の状態を判別するように構成される。

このような構成によって、しきい値を設定することにより、伝送信号の強度に応じて実効的な検出効率と誤り率とを自由に選ぶことが出来る。

また発明の量子暗号通信システムは、好ましくは、秘密鍵伝送のための位相変調の他に後から値の定まる位相変調を与えることによって外的な要因による参照信号と伝送信号との光路差の変動を補正するようにしている。

このような構成によって、秘密鍵伝送のための位相変調と後から定まる位相変調を与えることにより、光路差の変動の補正と量子状態の測定とを量子暗号と同時に行うことができる。

また本発明では、位相差が単調に増加する位相変調とランダムな位相変調とを

繰り返すことを特徴とする。このような構成により、光路差の変動の補正と量子状態の測定を同時に行うことができる。

またこの発明では、差信号の誤り率の増加に基づいて盗聴を検出することを特徴とする。このような構成により、盗聴の不適切な位相変調を行う確率の増加に基づき秘密鍵の誤り率が増加するため、盗聴の存在を検出することができる。

さらにこの発明では、差信号の量子力学的な状態を示すウィグナー分布関数の変化に基づいて盗聴を検出することを特徴とする。このような構成により、伝送信号の一部を分離して盗聴しても増幅過程が量子揺らぎを必ず伴うのでウィグナー分布関数の変化が生じる。したがって、ウィグナー分布関数の変化から盗聴を検出することができる。

また、本発明の量子暗号通信システムは、２つの出力光をフォトダイオードで電気変換することを特徴とする。このような構成により、高い量子効率でかつ十分なＳ／Ｎ比で信号の測定ができる。

さらに本発明の量子暗号通信システムは、光の波長が６００ｎｍ～９００ｎｍのときシリコンフォトダイオードを用い、光の波長が１０００ｎｍ～１５００ｎｍのときＩｎＧａＡｓフォトダイオードを用いることを特徴とする。このような構成により、高い量子効率と十分なＳ／Ｎ比で信号の測定ができる。

図面の簡単な説明

この発明は、以下の詳細な説明及び本発明の好ましい実施形態を示す添付図面により、より良く理解されるものとなろう。なお、添付図面に示す実施形態は本発明を特定又は限定することを意図するものではなく、単に本発明の説明及び理解を容易にするためのものである。

図中、

図１はこの発明の量子暗号通信システムの第１の実施形態の模式図である。

図２はこの発明の量子暗号通信システムにおける信号光の量子状態の揺らぎを考慮しない場合の受信者側の測定信号の模式図であり、（ａ）は参照光と信号光の経路の相対的な光路差とフォトダイオードに入射する光子数との関係図で、挿入図は光路差がゼロ付近の拡大図である。図２（ｂ）は参照光と信号光との差信

号を示す図である。

図３はこの発明における信号光の量子状態の揺らぎを考慮した場合の受信者側の測定信号の模式図で、（ａ）は光路差が０度の場合、（ｂ）は光路差が９０度（λ／４）の場合、（ｃ）は光路差が１８０度（λ／２）の場合、（ｄ）は光路差が２７０度（３λ／４）の場合であり、それぞれ横軸は差信号の大きさを示し、縦軸はその信号が検出される確率を示す。

図４は第１の実施形態の測定結果の例であり、（ａ）は５０００回測定したときの差信号の頻度分布図で、横軸は実際の測定電圧である。（ｂ）は（ａ）のような測定を３０回行って得たデータから計算機トモグラフィーにより求めた信号光のウィグナー分布関数の図である。

図５はこの発明による量子暗号の手順を示す図であり、左欄の１は送信者の位相変調、２は受信者の位相変調、３は送信者と受信者の位相変調の合計、４は受信者の測定結果、５は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、０度又は１８０度のとき○を、９０度又は２７０度のとき×を受信者に通知したこと、６は受信者が＋にビット１を、－にビット０を、○になった場合につき当てはめ秘密鍵としたこと、７は送信者が自分の位相変調が、０度又は９０度のときはビット１を、１８０度又は２７０度のときはビット０を当てはめ秘密鍵としたことを示す。

図６はこの発明の第２の実施形態の量子暗号装置の模式図である。

図７は第２の実施形態に位相変調を与える手順を示す表である。

発明を実施するための最良の形態

以下、図面に示した好適な実施形態に基づいて本発明を詳細に説明する。なお以下の説明では、本発明の例示的な実施形態について説明しているが、開示した実施形態に関して、本発明の要旨及び範囲を逸脱することなく、種々の変更、省略、追加が可能であることは当業者において自明である。したがって本発明は実施形態に限定されるものではなく、請求の範囲に記載された要素によって規定される範囲及びその均等範囲を包含するものとして理解されなければならない。

先ず本発明の量子暗号通信システムにおける典型的な第１の実施形態を図面を

参照して詳細に説明する。

図１は本発明による量子暗号通信システムの第１の実施形態の模式図である。図１を参照すると、本実施形態の量子暗号通信システムは、送信者の装置１０、伝送路１４，１６及び受信者の装置１２からなり、送信者の装置１０は、レーザー光源１と、ビームスプリッター２と、鏡３と、光減衰器４とを備えている。

レーザー光源１から出た光は、ビームスプリッター２で参照光Ｌと信号光Ｓとに分割される。信号光Ｓを反射する鏡３は光の波長程度の微少な距離の移動が可能で信号光Ｓの位相を変化させる。

信号光Ｓは光減衰器４により強度が減少し、典型的な強度が光子１個程度となるようにし、量子力学的な状態変化を検出できる微弱な信号にしている。

参照光Ｌの典型的な強度は光子１千万個程度であり、信号光Ｓと参照光Ｌの強度は著しく異なるように調節されている。

したがって、参照光Ｌの光の強度が信号光Ｓの光の強度よりも著しく大きいため、高効率の検出が可能になるとともに、信号光Ｓの量子状態の測定が可能になる。

受信者の装置１２は、光の波長程度の微少な距離の移動が可能な鏡５と、光の透過率と反射率とが等しいビームスプリッター６と、フォトダイオード７ａ，７ｂと、増幅器及び電圧測定器８とを備えている。

受信者は鏡５を移動することにより参照光Ｌと信号光Ｓとの相対的な位相差を変化させたあと、ビームスプリッター６上で２つの光を重ね合わせる。ビームスプリッター６からの２つの出力光はフォトダイオード７ａ，７ｂによりそれぞれ電気信号に変換する。さらに、その差信号を増幅し電圧を測定する。増幅器８にはチャージセンシティブアンプを用い、その典型的な利得は３０Ｖ／ｐＣ（ピコクーロン）なので、差信号に１万個の電子が含まれているときの出力電圧は５０ｍＶ程度となる。

フォトダイオードとしては波長が６００～９００ｎｍの光に対してはＳｉを、波長が１０００～１５００ｎｍの光に対してはＩｎＧａＡｓを使用すれば量子効率９０％以上、最適な場合では９９％以上の量子効率を実現できる。つまり、最適な場合、参照光Ｌの強度が強いということから例えば１万個の光子を９９００

個以上の電子に変換し、その電子数を十分なＳ／Ｎ比で測定することが可能である。

次に受信者の信号処理について説明する。以下の説明では簡単のためフォトダイオードの量子効率を１００％とし、また増幅器の雑音は無視できるとした。

図１を参照して、信号光Ｓと参照光Ｌはビームスプリッター２で分割された後、別の経路を通りビームスプリッター６上で重なり合うので、２つの経路の光路差により干渉を起こす。

ただし、２つの光の強度が著しく異なるので干渉稿の明瞭度は低い。

図２は信号光の量子状態の揺らぎを考慮しない場合の受信者側の測定信号の模式図であり、（ａ）は参照光と信号光の経路の相対的な光路差とフォトダイオードに入射する光子数との関係図であり、挿入図は光路差がゼロ付近の拡大図である。図２（ｂ）は参照光と信号光との差信号を示す図である。

図２（ａ）に示すように、ビームスプリッター６は信号光Ｓがないときに参照光Ｌを１対１に分割するよう調整するので、２つのフォトダイオード７ａ，７ｂに入射する光子数は共に参照光Ｌの光子数ｎ０ の半分程度である。それを中心として２つの経路の相対的な光路差に応じて微少な干渉稿が現れる。干渉稿の強弱は２つのフォトダイオード７ａ，７ｂで逆位相なので、両者の差信号をとると、図２（ｂ）に示すように干渉稿の部分のみを取り出すことができる。このとき干渉稿の振幅は信号光Ｓの光子数ｎ１ と参照光Ｌの光子数ｎ０ の積の平方根の２倍、すなわち２$\sqrt{n1}\sqrt{n0}$ である。なお、信号光Ｓと参照光Ｌの振幅は強度の平方根、つまり$\sqrt{n1}$ と$\sqrt{n0}$ であり、フォトダイオード７ａとフォトダイオード７ｂとの差の最大値は

$$\{(\sqrt{n1}+\sqrt{n0})^2/2-(\sqrt{n1}-\sqrt{n0})^2/2\}=2\sqrt{n1}\sqrt{n0}$$

となる。

さらに上述したのは多数回の平均値であり、１回ごとの差信号の測定結果には信号光Ｓの量子揺らぎにより標準偏差$\sqrt{n0}$ の揺らぎが存在する。

図３は信号光の量子状態の揺らぎを考慮した場合の受信者側の測定信号の模式図であり、（ａ）は光路差が０度の場合、（ｂ）は光路差が９０度（λ／４）の場合、（ｃ）は光路差が１８０度（λ／２）の場合、（ｄ）は光路差が２７０度

（３λ／４）の場合であり、それぞれ横軸は差信号の大きさを示し、縦軸はその信号が検出される確率を示す。

なおλは光の波長を示し、横軸は差信号を２√ｎ０ で割って規格化してある。

図３（ａ）に示すように、信号光Ｓと参照光Ｌとの相対的な光路差が０度の場合、信号光Ｓが平均光子数１のコヒーレント状態の場合に得られる差信号の頻度分布は平均値が１で、標準偏差が０．５のガウス分布となる。図３の（ｂ）～（ｄ）の場合は、平均値がそれぞれ０，－１，０となる。

したがって、量子暗号を実行するためには、受信者は１回ごとの測定について光路差が０度であったのか、あるいは１８０度であったのかを差信号の測定結果から判断することが可能になる。つまり、図３の（ａ）と（ｃ）とを区別すればよいので、しきい値Ｘ－、Ｘ＋を定めて、差信号がＸ＋以上であれば０度、Ｘ－以下であれば１８０度と判断することができる。

このように、Ｘ－とＸ＋とを設定することにより実効的な検出効率と誤り率を自由に設定できる。例えば図３のｎ１ ＝１の場合に、Ｘ－＝Ｘ＋＝０とすると、光路差が０度のときに０度と判断する確率（実効的な検出確率）は、ガウス分布を｛（平均値）－（標準偏差の２倍）｝から無限大まで積分すればよいので、９７．７％となる。逆に、光路差が１８０度であるのに０度と判断してしまう確率（誤り率）はガウス分布を｛（平均値）＋（標準偏差の２倍）｝から無限大まで積分したものなので２．２８％となる。またＸ－＝－０．５、Ｘ＋＝０．５とすると、同様の計算により実効的な検出確率が８４．１％まで低下するが、誤り率が０．１３％と非常に小さくなり、従来より優れた性能が得られる。

図４は第１の実施形態の測定結果の例であり、（ａ）は５０００回測定したときの差信号の頻度分布図で、横軸は実際の測定電圧である。（ｂ）は（ａ）のような測定を３０回行って得たデータから計算機トモグラフィーにより求めた信号光のウィグナー分布関数の図である。ウィグナー分布関数は信号光の量子状態の表現方法の一つであり、ウィグナー分布関数が得られたことは信号光の量子状態の測定が実際に可能であることを示している。

本実施形態の測定では５０００個の光パルスに対して差信号の電圧値を測定し頻度分布を求めたものであり、図４（ａ）に示すように頻度分布はガウス関数に

従っている。なお、図４（ａ）の横軸は実際の測定電圧であるので、分布の幅を図３の場合と直接比較するには、増幅器の利得と参照光の強度を使って補正する必要がある。

このような補正をすれば、測定された分布の幅（差信号の揺らぎの大きさ）は量子揺らぎで予測される幅と一致することが確かめられる。

図４（ｂ）は光路差を変化させながら５０００回の測定を３０組、計１５万パルス分のデータから求めたウィグナー分布関数である。

このように本発明の第１の実施形態では、光路差を変化させながら測定を行うことにより、信号光の量子力学的な状態の測定が可能である。ウィグナー分布関数は信号光について理論上知りうる全ての情報を含んでいるので、盗聴者の存在による信号光の変化を、より簡単に見いだすことが可能になる。

次に量子暗号の手順について説明する。

図５は本発明による量子暗号の手順を示す表であり、左欄の１は送信者の位相変調、２は受信者の位相変調、３は送信者と受信者の位相変調の合計、４は受信者の測定結果、５は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、０度又は１８０度のとき○を、９０度又は２７０度のとき×を受信者に通知したこと、６は受信者が＋にビット１を、－にビット０を、○になった場合につき当てはめ秘密鍵としたこと、７は送信者が自分の位相変調が、０度又は９０度のときはビット１を、１８０度又は２７０度のときはビット０を当てはめ秘密鍵としたことを示す。なお、ここでは簡単のため誤り率を０とする。

まず送信者は図１中の鏡３を制御することにより、０度、９０度、１８０度及び２７０度の位相の変化をランダムに信号光に加える（図５の左欄１）。一方受信者は鏡５により、０度又は９０度のランダムな位相変化を参照光に加える（同左欄２）。このとき合計の光路差は送信者と受信者の位相変調の差となる（同左欄３）。

さらに受信者は測定結果に対して、上述したＸ－、Ｘ＋の設定に従い、差信号がＸ－以下であれば「－」を、Ｘ＋以上であれば「＋」を割り当てる（同左欄４）。このとき左欄３が０度のときは必ず＋、１８０度のときは－、９０度と２７

０度のときは＋と－とが等確率で現れる（同左欄４）。

次に受信者はビットが０か１であった場合について、０度と９０度のどちらの位相変調を加えたかを例えば公衆回線を通じて送信者に連絡する（同左欄５）。

送信者は合計の光路差が０度か１８０度であったものについて、秘密鍵として採用することを受信者に連絡する。すなわち、送信者は位相変調の合計が０度又は１８０度のとき○を、９０度又は２７０度のとき×を受信者に通知する（同左欄５）。

受信者は＋にビット１を、－にビット０を、○となった場合につき当てはめ秘密鍵とする（同左欄６）。

そして送信者は自分の加えた位相変調が０度と９０度のものはビット１を、１８０度と２７０度のものはビット０を当てはめ秘密鍵とする（同左欄７）。

図５で示すように、このようにして生成された秘密鍵は送信者と受信者とで必ず一致する。

次に盗聴を知る方法を説明する。

量子的な測定は対象に必ず影響を及ぼすという原理により、第三者による盗聴の試みは伝送信号に必ず変化を与えるので、送信者と受信者とに気づかれずに第三者がこの秘密鍵を知ることは不可能である。

具体的な信号の変化は盗聴者がどのような手段をとるかに依存する。例えば盗聴者がいったん信号光を遮って情報を読み取り、受信者に信号を再送するという手段をとった場合、盗聴者の情報の読み取りに上述した受信者と同じ測定を行うとすると、誤った位相変調のときには（送信者の位相変調との合計が９０度や２７０度のとき）送信者の位相変調を知ることができず、受信者に正しい信号を再送することができない。

一般に互いに９０度離れた振幅成分の両方の情報を得ることは不確定性関係により不可能であるので、盗聴者がどのような手段で情報を読み取るとしても正しい情報は得られず、必ず誤り率の増加となって現れる。すなわち、送信者と受信者の秘密鍵が一致しない。例えば盗聴者が信号光をいったん遮って再送するという手段をとった場合は、不適切な位相変調を行う確率１／２と誤った信号を再送する確率１／２を掛け合わせた確率１／４で、送信者と受信者との秘密鍵が一致

しない。

したがって、秘密鍵の一部を照らし合わせることにより盗聴者の存在を検出することができる。

また信号光の一部を分離して測定して情報を部分的に得て、分離したことによる損失を増幅によって補うという盗聴手段の場合、従来の量子暗号では低い量子効率と相まって検出が困難であったが、本発明の場合ではウィグナー分布関数の変化となって現れるので受信者は直ぐ気が付くことになる。これは増幅過程が量子揺らぎの増減を必ず伴うので、図４（ａ）のような測定結果において分散の増減となって現れ、ウィグナー分布関数もピーク値のまわりの分布が全体的に太くなったり非対称となり、また盗聴者が確定的な情報を得た場合のみ増幅する盗聴手段をとった場合には、ピーク値をとるＸ１、Ｘ２の値も変化することになるからである。

次に、本発明の第２の実施形態について説明する。

この第２の実施形態は、伝送路として１本の光ファイバーを用いることを想定しており、上述した第１の実施形態のままでは困難である長距離の量子暗号を可能にするための実装である。そのために参照光と信号光とを時間及び偏光状態で分離し、同一の経路を伝送させるようにしたものであり、受信者の信号処理や量子暗号の手順は上述した第１の実施形態と同様である。

ただし、送信者と受信者との位相変調に量子暗号の手続に加え、別に予め定めた位相変調を与えることにより、光路差の安定性の改善と量子状態のモニターのための操作を加えている。

安定性の改善は、予め定めた位相変調の場合に予測される差信号と実際に測定される差信号との比較により行う。量子状態のモニターは一様に変化する位相変調を予め定めた位相変調として与えることにより実行できる。

図６は第２の実施形態の量子暗号装置の模式図である。

図６を参照すると、第２の実施形態は、送信者側に、直線偏光のパルス光を発生するレーザー光源２１と、このパルス光を２つに分割するビームスプリッター２２と、一方の経路の光、これを信号光として、信号光Ｓの偏光を９０度回転する半波長板２４と、吸収媒質により信号光Ｓの強度を弱くする光減衰器２５と、

信号光Ｓの位相を変化させる位相変調器２６と、他方の経路の光、これを参照光Ｌとして、この参照光Ｌと信号光Ｓとを同一光軸上に戻す偏光ビームスプリッター２３とを備え、参照光Ｌと信号光Ｓとを光ファイバー２７に入射するようになっている。このとき信号光Ｓと参照光Ｌとは互いに偏光が直交しており、かつ、時間的に離れた状態となっている。なお、図６中の１８，１９は鏡を示す。

光ファイバー２７の出力側には光ファイバー伝送中の偏光の乱れを補正する偏光素子２８が設けられている。本発明では参照光Ｌの強度が強いので、この参照光Ｌを用いて補正を行っている。

受信者側には、信号光Ｓと参照光Ｌとを分離する偏光ビームスプリッター２９と、先ほどとは逆に距離的に短い経路を通し途中で位相変化を信号光Ｓに与える位相変調器３０と、長い経路を通して参照光Ｌの偏光を９０度回転する半波長板３１と、参照光Ｌと信号光Ｓとを時間的及び偏光方向も一致させるビームスプリッター３２とを備え、このビームスプリッター３２からの参照光Ｌと信号光Ｓとをそれぞれフォトダイオード３３ａ、３３ｂにより電気信号に変化し、その差信号を増幅器及び電圧測定器３５で増幅し、電圧を測定するようになっている。なお、図６中の３８，３９は鏡を示す。

このような構成により、信号光Ｓと参照光Ｌとが異なる経路を進むのは送信者と受信者側の短い距離だけで、大部分の伝送路は同一の経路を進むので、２つの光の相対的な光路差の変動を小さくすることができる。

さらに相対的な光路差の変動の影響を除くために後から値の定まる位相変調と秘密鍵伝送のための位相変調とを与える。

図７はこの発明にかかる第２の実施形態に位相変調を与える手順を示す表である。

図７を参照してさらに説明すると、左欄の１は送信者の位相変調、アンダーラインのあるものは秘密鍵伝送のための位相変調、２は受信者の位相変調、３は送信者と受信者の位相変調の合計、４は受信者の測定結果、５は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、０度又は１８０度のとき○を、それ以外のときは合計の位相変調を受信者に通知したこと、６は受信者が＋にビット１を、－にビット０を、○になった場合につき当ては

め秘密鍵としたこと、７は送信者が自分の位相変調が、０度又は９０度のときはビット１を、１８０度又は２７０度のときはビット０を当てはめ秘密鍵としたことを示す。

後から定まる位相変調の場合（図７左欄５）は、差信号の平均値が予測できるので、逆に実際に測定される差信号の平均値から光路差の変動を見積もることができる。

したがって、たとえ外的な要因による相対的な光路差の変動があったとしても、その効果を打ち消すように補正することが可能になる。

さらにいろいろな位相での差信号のデータから計算機トモグラフィーにより信号光の量子状態を得ることができる。

したがって、本発明によれば、光路差の変動の補正と量子状態の測定を両方を同時に行うことが可能になる。

産業上の利用可能性

以上のように、本発明の量子暗号通信システムは伝送信号の量子力学的な状態の測定ができるとともに、実質的に高い量子効率で伝送信号の検出ができる。

したがって、本発明の量子暗号通信システムは第三者の盗聴が不可能な暗号通信システムとして極めて有用である。

請 求 の 範 囲

1．光信号を用いる量子暗号通信において、

盗聴の操作によって生じる信号光の差信号における振幅と位相とで規定される量子力学的な確率分布の変化に基づいて盗聴を検出することを特徴とする、量子暗号通信システム。

2．前記量子暗号通信において、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で上記参照信号と上記伝送信号とに位相差を付与し、これら２つの信号を受信側で重ね合わせて得られる相互に逆位相の関係にある２つの出力光の差を求め、上記伝送信号の量子状態の揺らぎに依存した上記出力光の差信号の頻度分布に基づいて送信側と受信側との秘密鍵を共有するとともに上記伝送信号の量子状態の揺らぎを直接測定するようにしたことを特徴とする、請求の範囲第１項に記載の量子暗号通信システム。

3．光源からの光を伝送信号と参照信号とに分割する第１のビームスプリッターと、上記伝送信号に位相変調を与える位相変調手段と、この伝送信号を量子力学的な状態変化で検出できる微弱な信号にする光減衰器と、上記参照信号に位相変調を与える位相変調手段とを備え、

上記伝送信号と参照信号とに相対的な位相差を付与後、

上記位相変調した微弱な伝送信号と上記位相変調した強度の強い参照信号とを重ね合わせ出力する第２のビームスプリッターと、この第２のビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、この第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有する、量子暗号通信システム。

4．前記位相変調手段が入射する光の波長程度の微小な距離を移動可能にした鏡

を含んでなることを特徴とする請求の範囲第３項に記載の量子暗号通信システム。

５．前記参照信号と前記伝送信号とを時間及び偏光状態で分離して同一の経路を伝送したことを特徴とする、請求の範囲第１～４項のいずれかに記載の量子暗号通信システム。

６．光源からの光を伝送信号と参照信号とに分割する第１のビームスプリッターと、上記伝送信号を一方の長い経路を通し偏光する第１の偏光素子と、この伝送信号を量子力学的な状態で検出できる微弱な信号にする光減衰器と、この伝送信号に所定の位相変調を与える第１の位相変調手段と、他方の短い経路に通した強度の強い上記参照信号と上記伝送信号とを同一光軸上に戻す第１の偏光ビームスプリッターとを備え、

上記伝送信号と参照信号とに相対的な位相差を付与後、

受信側にて一本の光ファイバーを伝送してきた上記伝送信号及び上記参照信号を分離する第２の偏光ビームスプリッターと、この分離した伝送信号を一方の短い経路に通し位相変調を与える第２の位相変調手段と、上記分離した参照信号を他方の長い経路に通し偏光する第２の偏光素子とを有しており、

時間及び偏光状態が一致した上記伝送信号と上記参照信号とを重ね合わせ出力する第２のビームスプリッターと、この第２のビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、この第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有する、量子暗号通信システム。

７．前記光ファイバーの出力側に前記参照信号の偏光の乱れを補正する第３の偏光素子を設けたことを特徴とする、請求の範囲第６項に記載の量子暗号通信システム。

８．前記差信号に正負それぞれにしきい値を設定し、このしきい値を基準にして

前記伝送信号の状態を判別することを特徴とする、請求の範囲第１～７項のいずれかに記載の量子暗号通信システム。

９．前記位相差の付与を秘密鍵伝送のための位相変調の他に後から値の定まる位相変調を与えることによって、外的な要因による前記参照信号と前記伝送信号との光路差の変動を補正することを特徴とする、請求の範囲第１～８項の何れかに記載の量子暗号通信システム。

１０．前記位相差が秘密鍵伝送のための位相変調と後から値の定まる位相変調とをランダムに繰り返すことを特徴とする、請求の範囲第１～９項のいずれかに記載の量子暗号通信システム。

１１．前記差信号の誤り率の増加に基づいて盗聴を検出することを特徴とする、請求の範囲第１～１０項のいずれかに記載の量子暗号通信システム。

１２．前記差信号の量子力学的な状態を示すウィグナー分布関数の変化に基づいて盗聴を検出することを特徴とする、請求の範囲第１～１１項のいずれかに記載の量子暗号通信システム。

１３．前記２つの出力光をフォトダイオードで電気変換することを特徴とする、請求の範囲第１～１２項の何れかに記載の量子暗号通信システム。

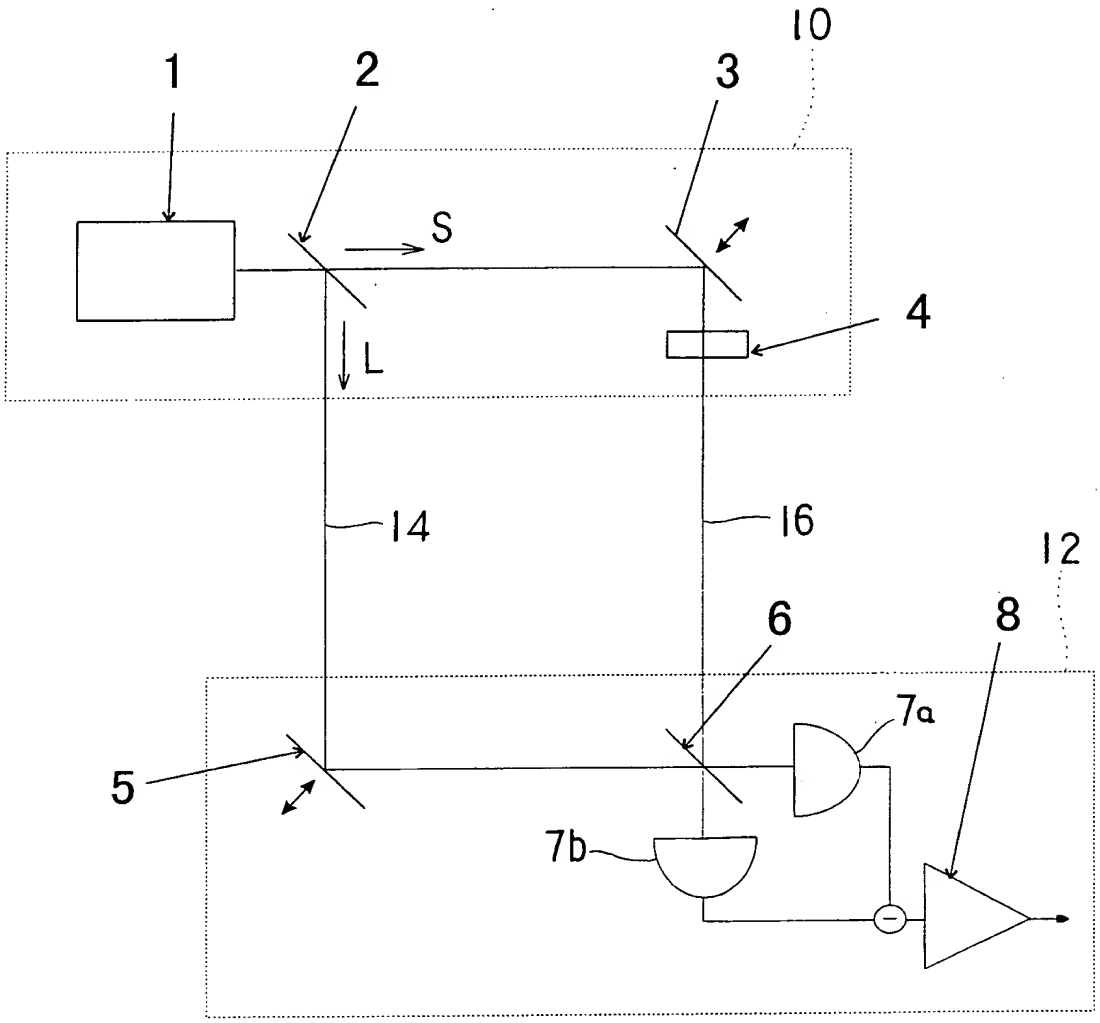
１４．光の波長が６００ｎｍ～９００ｎｍのときシリコンフォトダイオードを用い、光の波長が１０００ｎｍ～１５００ｎｍのときＩｎＧａＡｓフォトダイオードを用いることを特徴とする、請求の範囲第１～１３項の何れかに記載の量子暗号通信システム。

要 約 書

送信者はレーザー光源（１）と光減衰器（４）とを、受信者は増幅器及び電圧測定器（８）を備え、信号光（Ｓ）を反射する鏡（３），（５）は光の波長程度の微少な距離の移動が可能で信号光（Ｓ）の位相を変化させ、信号光（Ｓ）は光減衰器（４）により強度が減少し、典型的な強度が光子１個程度となるようにし、量子力学的な状態変化を検出できる微弱な信号にしている量子暗号通信システムである。

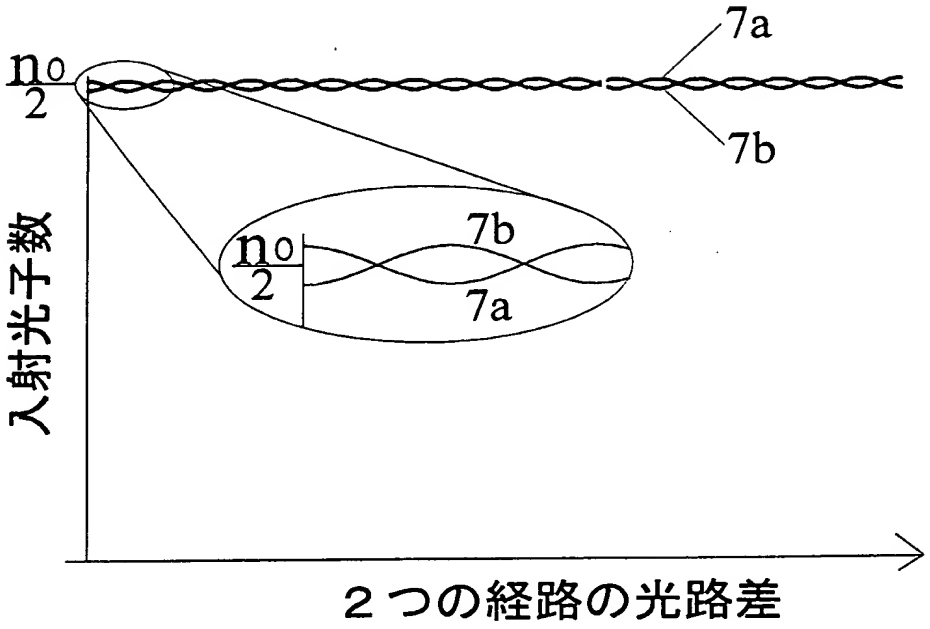
この量子暗号通信システムは第三者の盗聴が不可能な暗号通信システムとして極めて有用である。

【図　1】

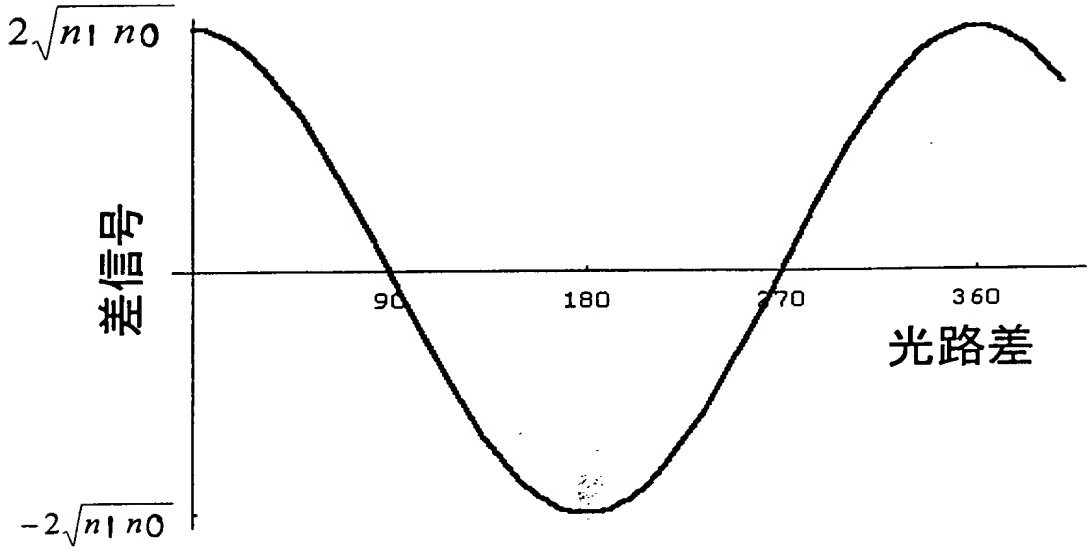


【図 2】

(a)

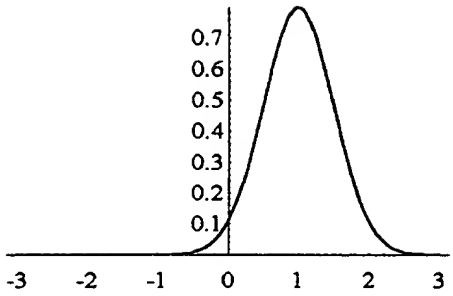

7a
$\frac{n_0}{2}$
7b
7b
$\frac{n_0}{2}$
7a
入射光子数
２つの経路の光路差

(b)

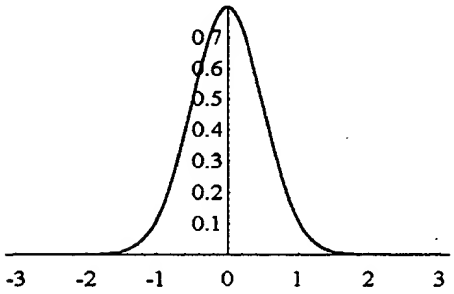

$2\sqrt{n_1 n_0}$
差信号
90
180
270
360
光路差
$-2\sqrt{n_1 n_0}$

【図 3】

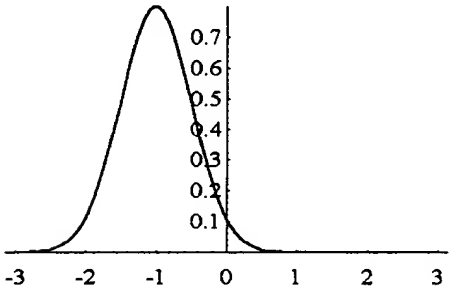
(a)


0.7
0.6
0.5
0.4
0.3
0.2
0.1
-3 -2 -1 0 1 2 3

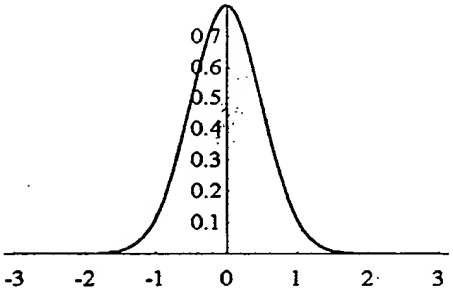
(b)


0.7
0.6
0.5
0.4
0.3
0.2
0.1
-3 -2 -1 0 1 2 3

(c)

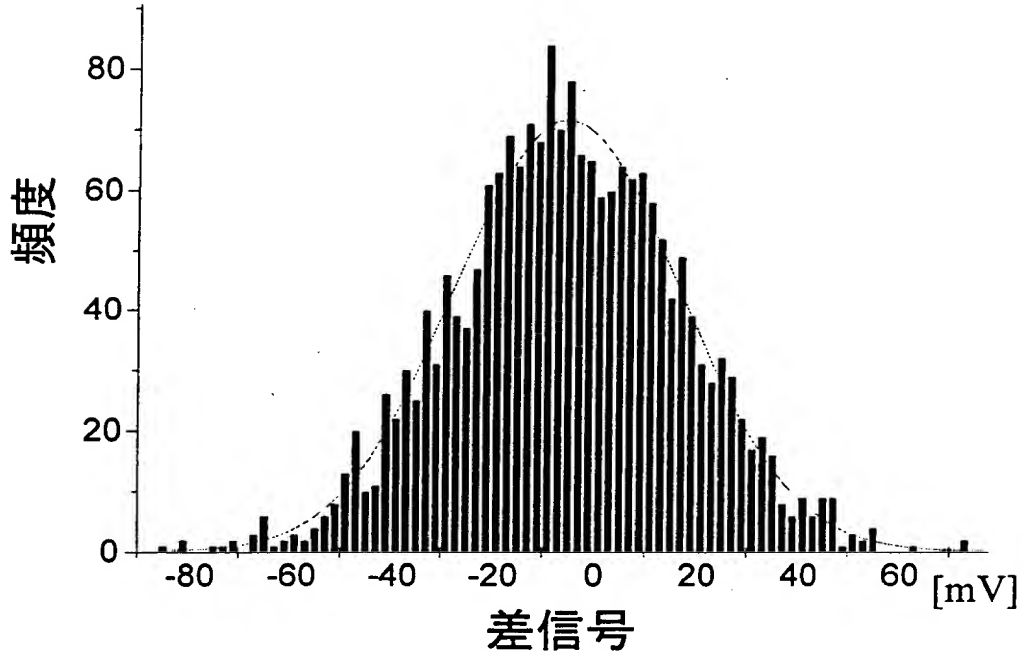

0.7
0.6
0.5
0.4
0.3
0.2
0.1
-3 -2 -1 0 1 2 3

(d)

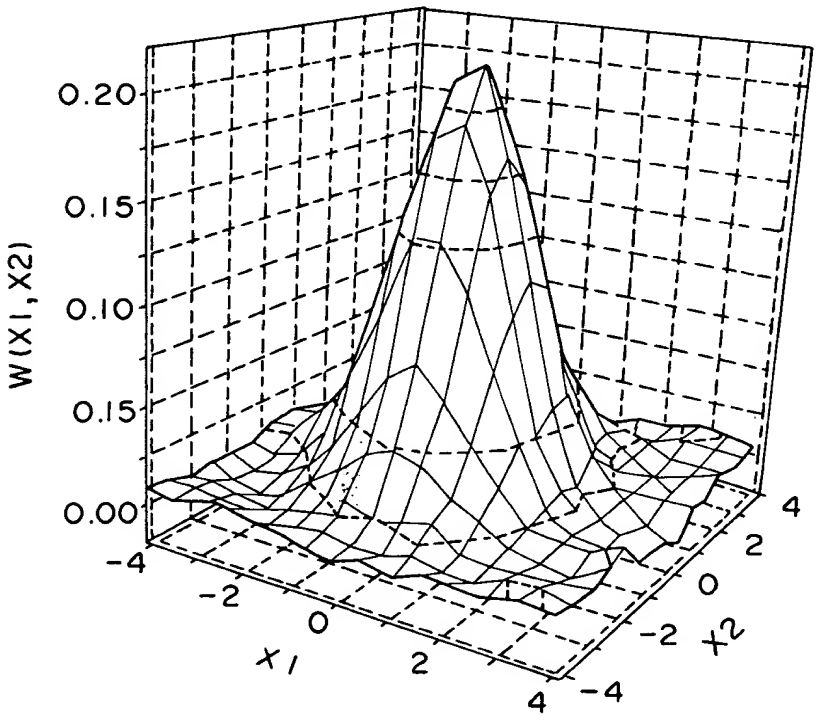

0.7
0.6
0.5
0.4
0.3
0.2
0.1
-3 -2 -1 0 1 2 3

【図 4】

(a)


頻度
80
60
40
20
0
-80
-60
-40
-20
0
20
40
60
[mV]
差信号

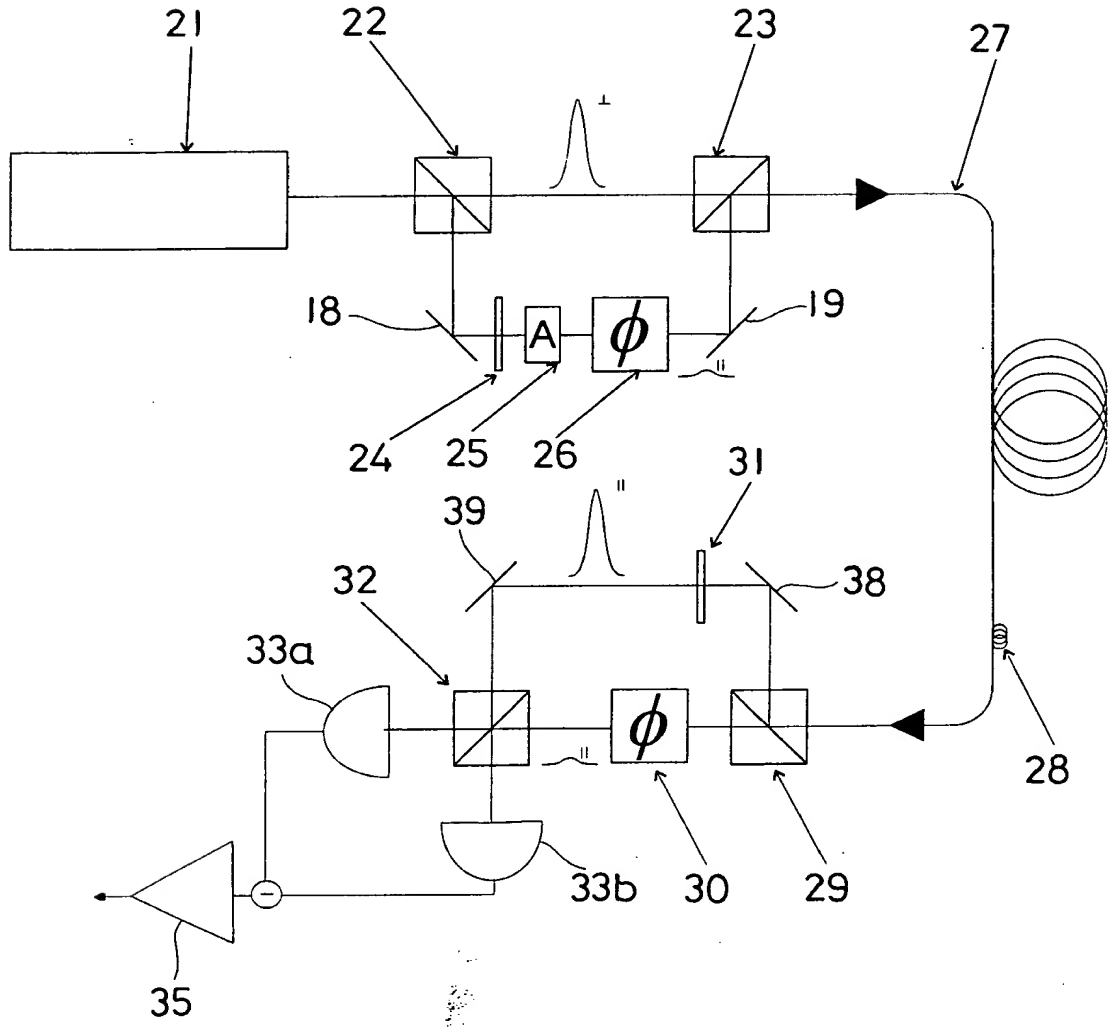
(b)


W(X1, X2)
0.20
0.15
0.10
0.15
0.00
-4
-2
0
2
4
X1
X2

【図 5】

1	270	90	180	90	270	90	270	0	90	180	90	270
2	0	90	90	0	0	90	90	0	90	90	0	90
3	270	0	90	90	270	0	180	0	0	90	90	180
4	+	+	—	+	+	+	—	+	+	+	—	—
5	×	○	×	×	×	○	○	○	○	×	×	○
6		1				1	0	1	1			0
7		1				1	0	1	1			0

【図 6】



【図 7】

1	100	180	90	150	90	130	120	90	180	160	270	70
2	0	90	90	0	0	90	90	90	0	90	90	90
3	100	90	0	150	90	40	30	0	180	70	180	340
4	+	—	+	—	+	+	—	+	—	+	—	—
5	100	90	○	150	90	40	30	○	○	70	○	340
6			1					1	0		0	0
7			1					1	0		0	0

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号　ＰＣＴ００１ＪＳＴ	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０４３２８	国際出願日 （日.月.年）　１０．０８．９９	優先日 （日.月.年）　２４．０９．９８
出願人（氏名又は名称） 平野　琢也		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　1　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号 PCT／JP99／04328

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl[6] H04L9／38, H04B10／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl[6] H04L9／38, H04B10／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922－1996
日本国公開実用新案公報 1971－1999
日本国登録実用新案公報 1994－1999
日本国実用新案登録公報 1996－1999

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	M. J. Werner, G. J. Milburn; "Eavesdropping using quanturn-nondemolition measurements", PHYSICAL REVIEW A, Vol. 47, No. 1 (1993) p. 639-641	1, 5, 8-11
Y		12-14
A		2-4, 6, 7
Y	H. Bartelt, K.-H. Brenner; "The Wigner Distribution Function An Alternate Signal Representation in Optics", ISRAEL Journal of TECHNOLOGY, Vol. 18, No. 5 (1980) p. 260-262	12

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
02. 11. 99	16.11.99

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	青木 重徳 印	5W 4229
	電話番号 03－3581－1101 内線 3576	

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	副島俊雄,貝淵俊二 著;新版・光ファイバ通信 株式会社電気通信技術ニュース社 発行,(12.12.1981) p.252-253	13,14
A	C.Marand, P.D.Townsend;"Quantum key distribution over distances as long as 30km.", Optics Letter,Vol.20,No.12 (1995) p.1695-1697	1-14
A	Yi Mu, Yuliang Zheng, Yan-Xia Lin;"Multi-User Quantum Cryptography", International Symposium on Information Theory & Its Application 1994,Vol.1 (1994) p.245-250	1-14
A	B.A.Slutsky, R.Rao, P.-C.Run, Y.Fainman; "Security of cryptography against individual attacks", PHYSICAL REVIEW A,Vol.57,No.4 (1998) p.2383-2398	1-14
A	松枝秀明;"量子暗号の現状と期待", 電子情報通信学会誌, Vol.81,No.3(25.03.1998) p.225-228	1-14